Google Inc. et al v. Egger et al
Doc. 441 Att. 18

Exhibit 19

Dockets.Justia.com

WSJ.com THE WALL STREET JOURNAL. ONLINE

FORMAT FOR PRINTING sponsored by

March 10, 2008

PAGE ONE

NSA's Domestic Spying Grows As Agency Sweeps Up Data

Terror Fight Blurs Line Over Domain; Tracking Email

By SIOBHAN GORMAN
March 10, 2008; Page A1

DOW JONES REPRINTS

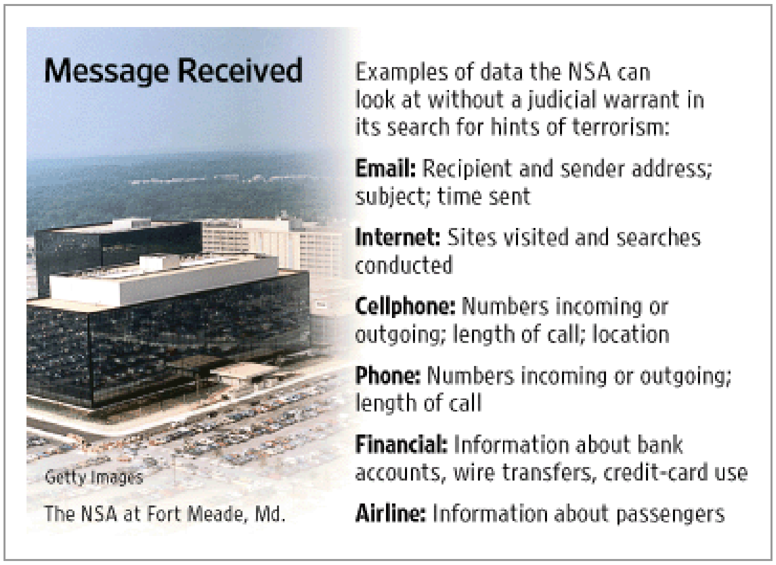
This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit: www.djreprints.com.

• See a sample reprint in PDF format.
• Order a reprint of this article now.

WASHINGTON, D.C. -- Five years ago, Congress killed an experimental Pentagon antiterrorism program meant to vacuum up electronic data about people in the U.S. to search for suspicious patterns. Opponents called it too broad an intrusion on Americans' privacy, even after the Sept. 11 terrorist attacks.

But the data-sifting effort didn't disappear. The National Security Agency, once confined to foreign surveillance, has been building essentially the same system.

The central role the NSA has come to occupy in domestic intelligence gathering has never been publicly disclosed. But an inquiry reveals that its efforts have evolved to reach more broadly into data about people's communications, travel and finances in the U.S. than the domestic surveillance programs brought to light since the 2001 terrorist attacks.


Message Received
Examples of data the NSA can look at without a judicial warrant in its search for hints of terrorism:
Email: Recipient and sender address; subject; time sent
Internet: Sites visited and searches conducted
Cellphone: Numbers incoming or outgoing; length of call; location
Phone: Numbers incoming or outgoing; length of call
Financial: Information about bank accounts, wire transfers, credit-card use
Airline: Information about passengers
Getty Images
The NSA at Fort Meade, Md.

Congress now is hotly debating domestic spying powers under the main law governing U.S. surveillance aimed at foreign threats. An expansion of those powers expired last month and awaits renewal, which could be voted on in the House of Representatives this week. The biggest point of contention over the law, the Foreign Intelligence Surveillance Act, is whether telecommunications and other companies should be made immune from liability for assisting government surveillance.

Largely missing from the public discussion is the role of the highly secretive NSA in analyzing that data, collected through little-known arrangements that can blur the lines between domestic and foreign intelligence gathering. Supporters say the NSA is serving as a key bulwark against foreign terrorists and that it would be reckless to constrain the agency's mission. The NSA says it is scrupulously following all applicable laws and that it keeps Congress fully informed of its activities.

According to current and former intelligence officials, the spy agency now monitors huge volumes of records of domestic emails and Internet searches as well as bank transfers, credit-card transactions, travel and telephone records. The NSA receives this so-called "transactional" data from other agencies or private companies, and its sophisticated software programs analyze the various transactions for suspicious patterns. Then they spit out leads to be explored by counterterrorism programs across the U.S. government, such as the NSA's own Terrorist Surveillance Program, formed to intercept phone calls and emails between the U.S. and overseas without a judge's approval when a link to al Qaeda is suspected.

The NSA's enterprise involves a cluster of powerful intelligence-gathering programs, all of which sparked civil-liberties complaints when they came to light. They include a Federal Bureau of Investigation program to track telecommunications data once known as Carnivore, now called the Digital Collection System, and a U.S. arrangement with the world's main international banking clearinghouse to track money movements.

The effort also ties into data from an ad-hoc collection of so-called "black programs" whose existence is undisclosed, the current and former officials say. Many of the programs in various agencies began years before the 9/11 attacks but have since been given greater reach. Among them, current and former intelligence officials say, is a longstanding Treasury Department program to collect individual financial data including wire transfers and credit-card transactions.

It isn't clear how many of the different kinds of data are combined and analyzed together in one database by the NSA. An intelligence official said the agency's work links to about a dozen antiterror programs in all.

A number of NSA employees have expressed concerns that the agency may be overstepping its authority by veering into domestic surveillance. And the constitutional question of whether the government can examine such a large array of information without violating an individual's reasonable expectation of privacy "has never really been resolved," said Suzanne Spaulding, a national-security lawyer who has worked for both parties on Capitol Hill.

NSA officials say the agency's own investigations remain focused only on foreign threats, but it's increasingly difficult to distinguish between domestic and international communications in a digital era, so they need to sweep up more information.

The Fourth Amendment

In response to the Sept. 11 attacks, then NSA-chief Gen. Michael Hayden has said he used his authority to expand the NSA's capabilities under a 1981 executive order governing the agency. Another presidential order issued shortly after the attacks, the text of which is classified, opened the door for the NSA to incorporate more domestic data in its searches, one senior intelligence official said.

Michael Hayden

The NSA "strictly follows laws and regulations designed to preserve every American's privacy rights under the Fourth Amendment to the U.S. Constitution," agency spokeswoman Judith Emmel said in a statement, referring to the protection against unreasonable searches and seizures. The Office of the Director of National Intelligence, which oversees the NSA in conjunction with the Pentagon, added in a statement that intelligence agencies operate "within an extensive legal and policy framework" and inform Congress of their activities "as required by the law." It pointed out that the 9/11 Commission recommended in 2004 that intelligence agencies analyze "all relevant sources of information" and share their databases.

Two former officials familiar with the data-sifting efforts said they work by starting with some sort of lead, like a phone number or Internet address. In partnership with the FBI, the systems then can track all domestic and foreign transactions of people associated with that item -- and then the people who associated with them, and so on, casting a gradually wider net. An intelligence official described more of a rapid-response effect: If a person suspected of terrorist connections is believed to be in a U.S. city -- for instance, Detroit, a community with a high concentration of Muslim Americans -- the government's spy systems may be directed to collect and analyze all electronic communications into and out of the city.

The haul can include records of phone calls, email headers and destinations, data on financial transactions and records of Internet browsing. The system also would collect information about other people, including those in the U.S., who communicated with people in Detroit.

The information doesn't generally include the contents of conversations or emails. But it can give such transactional information as a cellphone's location, whom a person is calling, and what Web sites he or she is visiting. For an email, the data haul can include the identities of the sender and recipient and the subject line, but not the content of the message.

Intelligence agencies have used administrative subpoenas issued by the FBI -- which don't need a judge's signature -- to collect and analyze such data, current and former intelligence officials said. If that data provided "reasonable suspicion" that a person, whether foreign or from the U.S., was linked to al Qaeda, intelligence officers could eavesdrop under the NSA's Terrorist Surveillance Program.

The White House wants to give companies that assist government surveillance immunity from lawsuits alleging an invasion of privacy, but Democrats in Congress have been blocking it. The Terrorist Surveillance Program has spurred 38 lawsuits against companies. Current and former intelligence officials say telecom companies' concern comes chiefly because they are giving the government unlimited access to a copy of the flow of communications, through a network of switches at U.S. telecommunications hubs that duplicate all the data running through it. It isn't clear whether the government or telecom companies control the switches, but companies process some of the data for the NSA, the current and former officials say.

An Intelligence Warehouse
1. Domestic agencies, including the departments of Justice, Homeland Security and Treasury, send information obtained under their surveillance programs to the National Security Agency.
2. The NSA, whose charter limits it to foreign spy activites, collects and analyzes this information with sophisticated software systems, where it sifts for patterns that could be related to a terror suspect or high-risk area.
3. The NSA feeds its findings into the effort the administration calls the Terrorist Surveillance Program and shares some of that information with other U.S. security agencies.
Travel
Communications
Money
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
E-mail
Web
Phone
Spending
Flights
Banking

On Friday, the House Energy and Commerce Committee released a letter warning colleagues to look more deeply into how telecommunications data are being accessed, citing an allegation by the head of a New York-based computer security firm that a wireless carrier that hired him was giving unfettered access to data to an entity called "Quantico Circuit." Quantico is a Marine base that houses the FBI Academy; senior FBI official Anthony DiClemente said the bureau "does not have 'unfettered access' to any communication provider's network."

The political debate over the telecom information comes as intelligence agencies seek to change traditional definitions of how to balance privacy rights against investigative needs. Donald Kerr, the deputy director of national intelligence, told a conference of intelligence officials in October that the government needs new rules. Since many people routinely post details of their lives on social-networking sites such as MySpace, he said, their identity shouldn't need the same protection as in the past. Instead, only their "essential privacy," or "what they would wish to protect about their lives and affairs," should be veiled, he said, without providing examples.

Social-Network Analysis

The NSA uses its own high-powered version of social-network analysis to search for possible new patterns and links to terrorism. The Pentagon's experimental Total Information Awareness program, later renamed Terrorism Information Awareness, was an early research effort on the same concept, designed to bring together and analyze as much and as many varied kinds of data as possible. Congress eliminated funding for the program in 2003 before it began operating. But it permitted some of the research to continue and TIA technology to be used for foreign surveillance.

Some of it was shifted to the NSA -- which also is funded by the Pentagon -- and put in the so-called black budget, where it would receive less scrutiny and bolster other data-sifting efforts, current and former intelligence officials said. "When it got taken apart, it didn't get thrown away," says a former top government official familiar with the TIA program.

Two current officials also said the NSA's current combination of programs now largely mirrors the former TIA project. But the NSA offers less privacy protection. TIA developers researched ways to limit the use of the system for broad searches of individuals' data, such as requiring intelligence officers to get leads from other sources first. The NSA effort lacks those controls, as well as controls that it developed in the 1990s for an earlier data-sweeping attempt.

Sen. Ron Wyden, an Oregon Democrat and member of the Senate Intelligence Committee who led the charge to kill TIA, says "the administration is trying to bring as much of the philosophy of operation Total Information Awareness as it can into the programs they're using today." The issue has been overshadowed by the fight over telecoms' immunity, he said. "There's not been as much discussion in the Congress as there ought to be."

Opportunity for Debate

But Sen. Kit Bond of Missouri, the ranking Republican on the committee, said by email his committee colleagues have had "ample opportunity for debate" behind closed doors and that each intelligence program has specific legal authorization and oversight. He cautioned against seeing a group of intelligence programs as "a mythical 'big brother' program," adding, "that's not what is happening today."

READ THE RULING

While the Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," the legality of data-sweeping relies on the government's interpretation of a 1979 Supreme Court ruling allowing records of phone calls -- but not actual conversations -- to be collected without a warrant. Read the ruling.[1]

The legality of data-sweeping relies largely on the government's interpretation of a 1979 Supreme Court ruling allowing records of phone calls -- but not actual conversations -- to be collected without a judge issuing a warrant. Multiple laws require a court order for so-called "transactional'" records of electronic communications, but the 2001 Patriot Act lowered the standard for such an order in some cases, and in others made records accessible using FBI administrative subpoenas called "national security letters." (Read the ruling.[2])

A debate is brewing among legal and technology scholars over whether there should be privacy protections when a wide variety of transactional data are brought together to paint what is essentially a profile of an individual's behavior. "You know everything I'm doing, you know what happened, and you haven't listened to any of the contents" of the communications, said Susan Landau, co-author of a book on electronic privacy and a senior engineer at Sun Microsystems Laboratories. "Transactional information is remarkably revelatory."

Ms. Spaulding, the national-security lawyer, said it's "extremely questionable" to assume Americans don't have a reasonable expectation of privacy for data such as the subject-header of an email or a Web address from an Internet search, because those are more like the content of a communication than a phone number. "These are questions that require discussion and debate," she said. "This is one of the problems with doing it all in secret."

Gen. Hayden, the former NSA chief and now Central Intelligence Agency director, in January 2006 publicly defended the activities of the Terrorist Surveillance Program after it was disclosed by the New York Times. He said it was "not a driftnet over Lackawanna or Fremont or Dearborn, grabbing all communications and then sifting them out." Rather, he said, it was carefully targeted at terrorists. However, some intelligence officials now say the broader NSA effort amounts to a driftnet. A portion of the activity, the NSA's access to domestic phone records, was disclosed by a USA Today article in 2006.

The NSA, which President Truman created in 1952 through a classified presidential order to be America's ears abroad, has for decades been the country's largest and most secretive intelligence agency. The order confined NSA spying to "foreign governments," and during the Cold War the NSA developed a reputation as the world's premier code-breaking operation. But in the 1970s, the NSA and other intelligence agencies were found to be using their spy tools to monitor Americans for political purposes. That led to the original FISA legislation in 1978, which included an explicit ban on the NSA eavesdropping in the U.S. without a warrant.

Big advances in telecommunications and database technology led to unprecedented data-collection efforts in the 1990s. One was the FBI's Carnivore program, which raised fears when it was in disclosed in 2000 that it might collect telecommunications information about law-abiding individuals. But the ground shifted after 9/11. Requests for analysis of any data that might hint at terrorist activity flooded from the White House and other agencies into NSA's Fort Meade, Md., headquarters outside Washington, D.C., one former NSA official recalls. At the time, "We're scrambling, trying to find any piece of data we can to find the answers," the official said.

The 2002 congressional inquiry into the 9/11 attacks criticized the NSA for holding back information, which NSA officials said they were doing to protect the privacy of U.S. citizens. "NSA did not want to be perceived as targeting individuals in the United States" and considered such surveillance the FBI's job, the inquiry concluded.

FBI-NSA Projects

The NSA quietly redefined its role. Joint FBI-NSA projects "expanded exponentially," said Jack Cloonan, a longtime FBI veteran who investigated al Qaeda. He pointed to national-security letter requests: They rose from 8,500 in 2000 to 47,000 in 2005, according to a Justice Department inspector general's report last year. It also said the letters permitted the potentially illegal collection of thousands of records of people in the U.S. from 2003-05. Last Wednesday, FBI Director Robert Mueller said the bureau had found additional instances in 2006.

It isn't known how many Americans' data have been swept into the NSA's systems. The Treasury, for instance, built its database "to look at all the world's financial transactions" and gave the NSA access to it about 15 years ago, said a former NSA official. The data include domestic and international money flows between bank accounts and credit-card information, according to current and former intelligence officials.

The NSA receives from Treasury weekly batches of this data and adds it to a database at its headquarters. Prior to 9/11, the database was used to pursue specific leads, but afterward, the effort was expanded to hunt for suspicious patterns.

Through the Treasury, the NSA also can access the database of the Society for Worldwide Interbank Financial Telecommunication, or Swift, the Belgium-based clearinghouse for records of international transactions between financial institutions, current and former officials said. The U.S. acknowledged in 2006 that the CIA and Treasury had access to Swift's database, but said the NSA's Terrorism Surveillance Program was separate and that the NSA provided only "technical assistance." A Treasury spokesman said the agency had no comment.

Through the Department of Homeland Security, airline passenger data also are accessed and analyzed for suspicious patterns, such as five unrelated people who repeatedly fly together, current and former intelligence officials said. Homeland Security shares information with other agencies only "on a limited basis," spokesman Russ Knocke said.

NSA gets access to the flow of data from telecommunications switches through the FBI, according to current and former officials. It also has a partnership with FBI's Digital Collection system, providing access to Internet providers and other companies. The existence of a shadow hub to copy information about AT&T Corp. telecommunications in San Francisco is alleged in a lawsuit against AT&T filed by the civil-liberties group Electronic Frontier Foundation, based on documents provided by a former AT&T official. In that lawsuit, a former technology adviser to the Federal Communications Commission says in a sworn declaration that there could be 15 to 20 such operations around the country. Current and former intelligence officials confirmed a domestic network of hubs, but didn't know the number. "As a matter of policy and law, we can not discuss matters that are classified," said FBI spokesman John Miller.

The budget for the NSA's data-sifting effort is classified, but one official estimated it surpasses $1 billion. The FBI is requesting to nearly double the budget for the Digital Collection System in 2009, compared with last year, requesting $42 million. "Not only do demands for information continue to increase, but also the requirement to facilitate information sharing does," says a budget justification document, noting an "expansion of electronic surveillance activity in frequency, sophistication, and linguistic needs."

Write to Siobhan Gorman at siobhan.gorman@wsj.com[3]

URL for this article:
http://online.wsj.com/article/SB120511973377523845.html

Hyperlinks in this Article:
(1) http://supreme.justia.com/us/442/735/case.html
(2) http://supreme.justia.com/us/442/735/case.html
(3) mailto:siobhan.gorman@wsj.com

Copyright 2008 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our **Subscriber Agreement** and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit **www.djreprints.com**.

RELATED ARTICLES FROM ACROSS THE WEB

More related content *Powered by Sphere*